AMENDMENTS TO THE DRAWINGS

Applicant has amended FIGs. 6-10 to include the legend "Prior Art." No new matter has been added.

The attached replacement sheets designated as FIGs. 6-10 replace the original sheets designated as FIGs. 6-10.

REMARKS

In the Official Action mailed on **23 August 2005** the Examiner reviewed claims 67-70. The abstract was objected to for being too long. The drawings were objected to. Claims 67 and 69 were objected to under 35 U.S.C. §101 because they are directed to non-statutory subject matter. Claims 69-70 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gligor (USPub 2001/0033656, hereinafter "Gligor") in view of Jutla (*Encryption Modes with Almost Free Message Integrity*, August 2000, hereinafter "Jutla"), in further view of Menezes, (*Handbook of Applied Cryptography*, 1997, hereinafter "Menezes").

Objection to the Abstract

The abstract was objected to for being too long.

Applicant has supplied a new Abstract that is within the 150 word limit. No new matter has been added.

Objections to the Drawings

The drawings were objected to because FIGs. 6-10 were not marked as "prior art."

Applicant has amended FIGs. 6-10 to include the proper markings. No new matter has been added.

Rejections under 35 U.S.C. §101

Claims 67 and 69 were objected to because they are directed to non-statutory subject matter.

Applicant has amended claims 67 and 69 to incorporate the suggestions of the Examiner.

Rejections under 35 U.S.C. §103(a)

Claims 69-70 were rejected as being unpatentable over Gligor in view of Jutla in further view of Menezes.

Applicant respectfully disagrees that claims 69-70 are obvious in view of Gligor, Jutla, and Menezes. A paper by the Applicant on offset codebook (OCB) encryption was accepted into a competitive conference on cryptography, *The 8th ACM Conference on Computer and Communications Security* (commonly referred to as the ACM CCS conference), a well-regarded venue with an acceptance rate (for the year in question, 2001) of 18%. The paper's only significant contribution is the OCB scheme—the same scheme that is narrowly described by claims 69-70. The OCB scheme is clearly described in the ACM CCS paper as being an improvement to the work of Gligor and Jutla, work that was known in the inventor's community at the time of the ACM CCS submission and was clearly referenced in the paper. If the cryptographic community viewed the subject claims as obvious in view of Gligor and Jutla and Menezes, the paper would most certainly not have been accepted. A copy of the inventor's ACM CCS paper is included with this response.

The inventor's ACM CCS paper above was regarded as one of the top papers at the conference and was therefore invited to a well-respected journal, *ACM Transactions on Information and Systems Security* (ACM TISSEC), where it underwent additional review and subsequently appeared. If the inventor's community viewed the subject claims as obvious in view of Gligor, Jutla, and Menezes, the paper would not have been invited into a well-regarded journal. The inventor's ACM TISSEC paper is included with this response.

Additionally, the commercial community has already decided that OCB is non-obvious: the method has been licensed multiple times, yielding 6-figure earnings, to medium and large companies. The attorneys at these companies know that there is pending IP of Gligor and Jutla (both VDG Inc. and IBM have made public disclosures in connection with activities at NIST, the IEEE, and other

venues) and yet they have chosen to license OCB, never expressing any concern that the patent claims would be seen as obvious given prior work. A declaration under 37 C.F.R. 1.132 and copies of three licensing agreements establishing the commercial success of the invention are attached to this amendment. Applicant considers the licensing agreements to be proprietary and requests that the licensing agreements be held in confidence in accordance with MPEP 724.02

The Applicant, knowing intimately the contents of Gligor et al and Jutla and the book by Menezes et al, spent months of intensive effort to develop the disclosed methods, as narrowly defined by the subject claims. Many attempts failed: there were 14 unpublished versions of OCB, many of which had subtle bugs that took weeks to discover by the inventor or the coauthors of his papers. The inventor and his coauthors are of more than ordinary skill in the art; the inventor is a well-known cryptographer with more than 3000 references to his papers, and the winner of the RSA Prize in Mathematics. He did not find the method described by the claims as obvious, nor did co-author Mihir Bellare, who is widely regarded as the top cryptographer of his generation.

Gligor's patent application makes clear that his only idea for handling messages that were not a multiple of the block length was to use padding (e.g., 10* pad the final block to make it a multiple of the block length, and then continue by using the padded message). Gligor's patent application mentions no less than *seven times* that messages that have a length other than the block length are to be padded as necessary to get them to be a multiple of the block length. No other approach is mentioned, and, in fact, padding is the only obvious approach to correctly deal with this issue. It was a first goal of the subject patent application to deal with messages that are not a multiple of the block length by a method smarter than the obvious padding approach: messages not a multiple of the block length are *not* padded in the disclosed technique.

Alternatives to padding that one might initially think of do not work because they break the authenticity protection in subtle ways. This is true for

many other potential refinements to the schemes of Jutla and Gligor et al, too. As explained in the ACM CCS paper, "We have found schemes of this sort to be amazingly "fragile"—tweak them a little and they break." Representative examples of such breaks are given the "Definition of the checksum" paragraph and the "Avoiding pretag collisions" paragraphs on pp. 201-202 of the inventor's ACM CCS paper. Applicant maintains that a method is non-obvious when schemes that are very close to it have subtle errors.

Jutla and Gligor et al provided to NIST the most efficient schemes they knew how to construct. Their proposals are less efficient than OCB according to multiple metrics, as described in the descriptive portion of the subject patent application. It is not reasonable to assume that Jutla or Gligor themselves regarded as obvious the techniques described in the pending patent application that could have made their proposals more efficient.

There are technical difficulties with the Examiner's reading of claims 69-70 against Gligor, Jutla, and Menezes. In particular, items (h) and (j) on p. 5 of the Examiner's office action are not analogous to Menezes p. 340, while item (k) is not analogous to Gligor [0025]. Regarding (h) and (j), the examiner's refers to the Matyas-Meyer-Oseas hash function, a classical method to construct a hash function from a block cipher. There is no length-encoding used in this hash function, and there is no xoring of a portion of a block cipher output with a string having length possibly less than the length of the block cipher. It is simply a chaining method, like CBC encryption. As for item (k), Gligor [0025] mentions padding in an unrelated context—as a way to ensure that all messages acted on in Gligor's scheme have length that is a multiple of n bits (denoted as "I" bits by Gligor). Such padding aims to solve a problem solved by the current patent application—handling messages that are not a multiple of the block size—but it does so at a cost of longer ciphertexts. The padding in (k) of the patent application is taking a fragment (something less than n bits) and adding bits (e.g. 0-bits) simply in order to feed it into the checksum calculation—a checksum

calculation that would not work correctly if, for example, a padded message fragment were directly used. This is unrelated to Gligor's initial padding of the input message where he aims to avoid otherwise dealing with "peculiar-length" strings.

Finally, Applicant comments that in providing a block-cipher-based cryptographic mode of operation (whether for encryption, message authentication, authenticated encryption, collision-intractable hashing, or some other end), anything one does is going to be a combining of basic building blocks (apply the block cipher, xor the following words, partition a message, add some padding, combine the following strings, and so forth). The non-obvious part is finding the right way to combine basic operational elements in order to more simply and efficiently accomplish some cryptographic task. In this domain, specious approaches are common and finding a correct way to meld basic building blocks can be highly non-obvious.

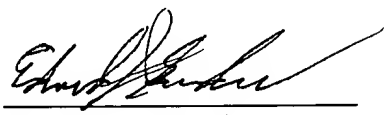
Applicant has amended claims 69 and 70 to clarify that the present invention encrypts messages of arbitrary length into a ciphertext of the same length. These amendments find support on page 24, line 32 to page 25, line 7 of the instant application.

Hence, Applicant respectfully submits that independent claims 67-70 are in condition for allowance.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47,615

Date: 23 November 2005

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com